Forensic Challenge V2.0

UNAM-CERT
RedIRIS

Topics

* Forensic Challenge V1.0

* Forensic Challenge V2.0

* Conclusions

Introduction

Why this forensic Challenge ?

* To promote and impulse the Forensic Analysis in our Region --Hispanoamerica--

* To know which tools are being used by our communitty in the Academy, Private and Public sector

* In order to count with a simple picture of this area, research, etc.

Forensic Challenge V1.0

Organized in 2003 by RedIRIS, in collaboration with:

- * UNAM-CERT (México)
- * CAIS/RNP (Brasil)
- * SANS
- * Spanish Security Experts

* Awards donated from some companies:

- * Encase (Guidance Software)
- * SANS documentation

* Forensic analysis of a compromised Linux Machine (Honeypot)

- * No special intrusion, simple one.

* Small diffusion security lists in Spanish

Forensic Challenge V1.0

Objective:

* Promote computer forensic “awareness” in our constituencies
* Provide a “learn by example” repository of forensic analysis in

Spanish that could be useful to users that want to learn about computer forensic.

At the end: 14 participants send their reports that are published in the web pages

High quality of all the reports

Forensic Challenge V1.0

Participants must present:

* Anonymous “executive” report describing the incident.
* Technical report (60 pages max.) analyzing the incident.

It was very important that the report describes not only what the intruder has done, but also how the forensic expert has found it:

* Describing the tools used in the analysis .
* Correlating information from different sources.

Forensic Challenge V1.0

* All reports obtained more than 5 points (if use a scale of 10 point for the best papers, the “fewer” was 6,2 points).

* Most users provided graph and statistics of the intrusion
Different techniques and tools used:

* Sleutkit
* TCT

But also :

- Home made tools Home made tools
- Repositories of MD5 files Repositories of MD5 files

* BSD accounting from the compromised system
* SWAP memory cumps

Forensic Challenge V2.0

* Launched last December 8th 2004.

* Promoted this year by UNAM-CERT (México), with some help from RedIRIS, CAIS-RNP.

    * Published in many Security list and also in the media newspapers, TV, etc.

    * Ask people to register to know the number of people interested in this challenge

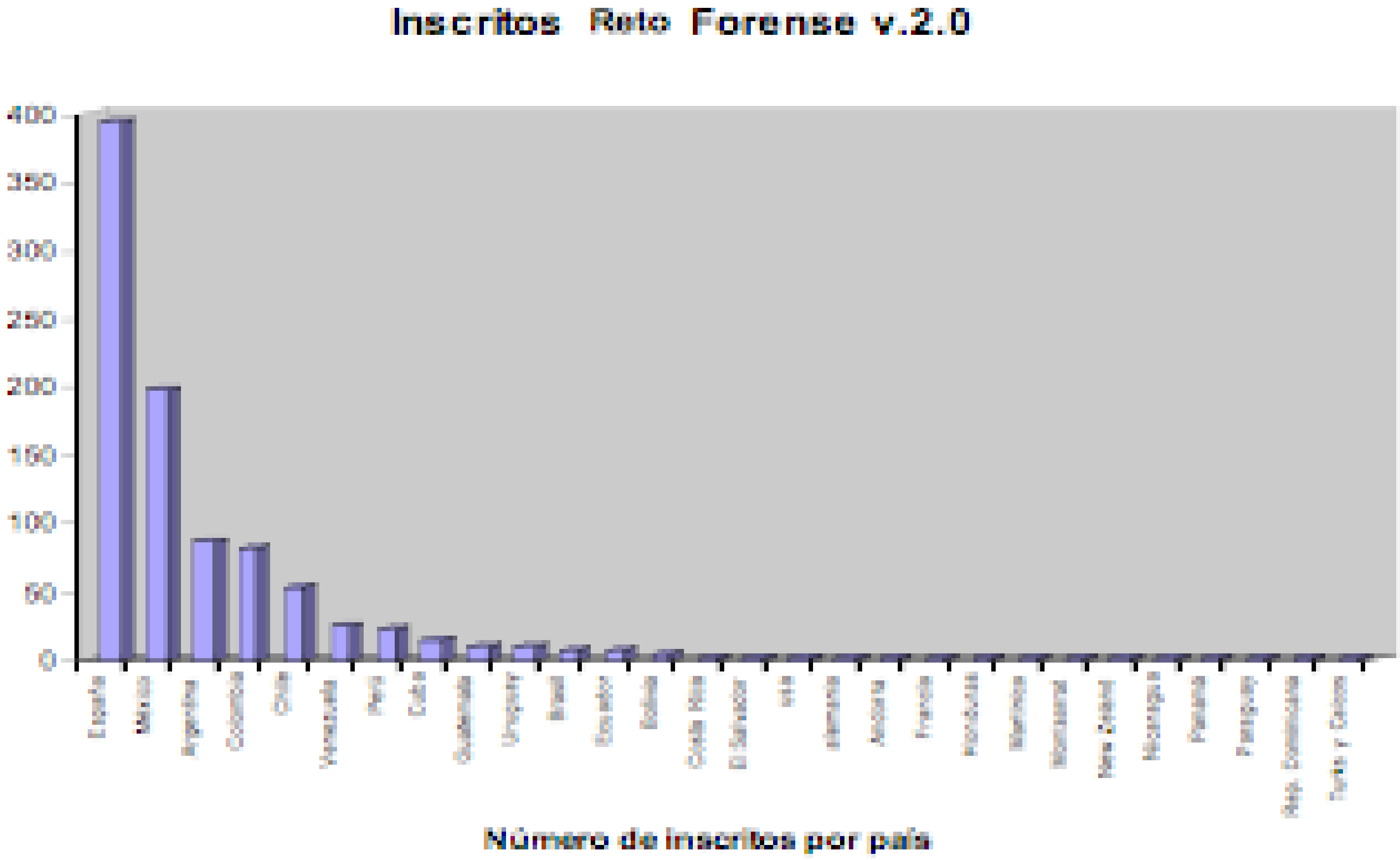
The Challenge started on 1st of February 2005

Forensic Challenge V2.0

For this Forensic challenge, registered almost 1000 participants from 26 different countries:

- España
- México
- Argentina
- Colombia
- Chile
- Venezuela

Forensic Challenge V2.0



Forensic Challenge V2.0

Forensic Analysis of a compromised Linux Machine

* Recovered from a Honeypot at UNAM-CERT

* Red Hat 7.3

* Khaos User

* It was very complex to analyze and present the final report.

* A lot of participants didn´t finishes because of complexity of the case

Forensic Challenge V2.0

Conclusions:

Almost all of our participants used Unix tools except one, who used Encase Forensic tools on a Windows Machine.

Most used tools were:

- Sleuthkit
- Autopsy
- Chkrootkit
- Rkhunter
- Unix Tools(grep, awk, etc.)

Forensic Challenge V2.0

Conclusions:

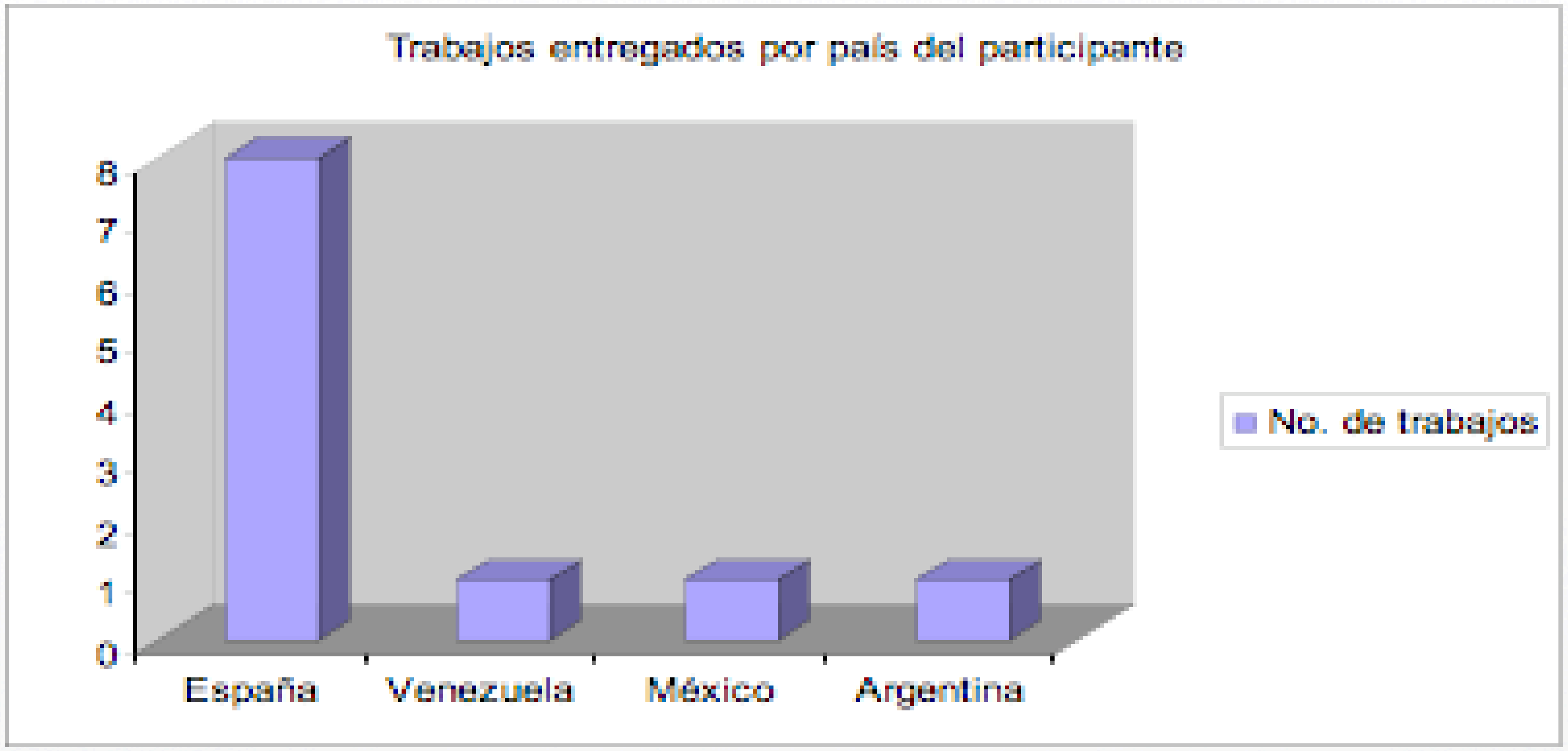
* To emphasize that 3rd place (Juan Antonio Fernández Gómez) used only a Unix tools.

* It's important to stand out that there is a difference between Forensic Analysis communitty from Spain respect the others in order to present reports, tools used, etc.

* From 11 reports 8 were from spain, 1 from Mexico, 1 from Venezuela and the lasst one from Argentina.

Forensic Challenge V2.0

Conclusions:



Forensic Challenge V2.0

Conclusions:

* We can conclude that Spain community has more human resources working on this area, Neverthless we saw an important increase and interest from our community for the next challenge.

2 Mailing list has been created due this purpose and the participants exchange some information, tools, ideas, etc which we hope this impulse this area in our community.

Forensic Challenge V2.0

Conclusions:

Several problems were detected in the course of Forensic Challenge like:

* Image size too large 10 GB.

* For the first two days images were only at UNAM, we need it a Mirror in Spain.

* The necessity to count with a pre defined format due diversity of criteria in order to evaluate certains aspects of the challenge.

Forensic Challenge V2.0

Challenges for the Forensic Challenge

- * Standardized format for the final report
- * Traffic Analysis for the Jury
- * Working closely with the participants, community and sponsors

Forensic Challenge V2.0

Forensic Challenge V3.0 ????

¿¿Preguntas??

http://www.seguridad.unam.mx

http://www.rediris.es/